



JN0-333^{Q&As}

Security, Specialist (JNCIS-SEC)

Pass Juniper JN0-333 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/jn0-333.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Click the Exhibit button.

```
[edit]
user@host# show security policies
from-zone red to-zone blue {
    policy deny-http {
        match {
            source-address any;
            destination-address any;
            application junos-https;
        }
        then {
            deny;
        }
    }
}
from-zone red to-zone blue{
    policy default-permit {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}

[edit]
user@host# run show security flow status
Flow forwarding mode:
Inet forwarding mode: packet based (reboot needed to change to flow based)
Inet6 forwarding mode: drop
MPLS forwarding mode: drop
ISO forwarding mode: drop
Flow trace status
Flow tracing status: off
Flow session distribution
Distribution mode: RR-based
Flow ipsec performance acceleration: off
Flow packet ordering
Ordering mode: Hardware
```

You notice that your SRX Series device is not blocking HTTP traffic as expected. Referring to the exhibit, what should you do to solve the problem?

- A. Commit the configuration.
- B. Reboot the SRX Series device.
- C. Configure the SRX Series device to operate in packet-based mode.



D. Move the deny-http policy to the bottom of the policy list.

Correct Answer: B

QUESTION 2

You recently configured an IPsec VPN between two SRX Series devices. You notice that the Phase 1 negotiation succeeds and the Phase 2 negotiation fails.

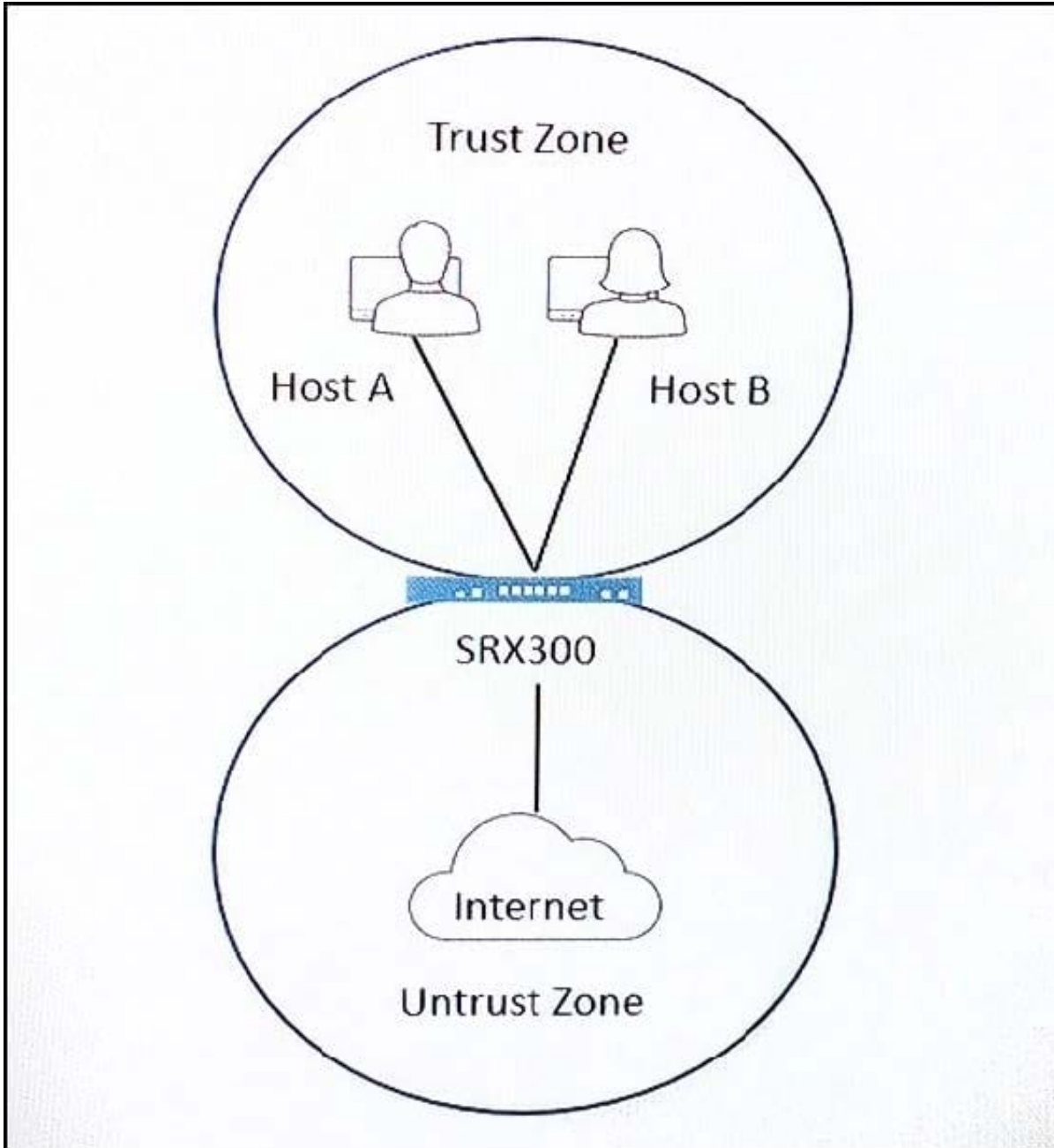
Which two configuration parameters should you verify are correct? (Choose two.)

- A. Verify that the IKE gateway proposals on the initiator and responder are the same.
- B. Verify that the VPN tunnel configuration references the correct IKE gateway.
- C. Verify that the IPsec policy references the correct IKE proposals.
- D. Verify that the IKE initiator is configured for main mode.

Correct Answer: AC

QUESTION 3

Click the Exhibit button.



You are monitoring traffic, on your SRX300 that was configured using the factory default security parameters. You notice that the SRX300 is not blocking traffic between Host A and Host B as expected.

Referring to the exhibit, what is causing this issue?

- A. Host B was not assigned to the Untrust zone.
- B. You have not created address book entries for Host A and Host B.
- C. The default policy has not been committed.
- D. The default policy permits intrazone traffic within the Trust zone.

Correct Answer: D



QUESTION 4

You must verify if destination NAT is actively being used by users connecting to an internal server from the Internet.

Which action will accomplish this task on an SRX Series device?

- A. Examine the destination NAT translations table.
- B. Examine the installed routes in the packet forwarding engine.
- C. Examine the NAT translation table.
- D. Examine the active security flow sessions.

Correct Answer: A

QUESTION 5

Click the Exhibit button.



```
[edit]
user@host# show security address-book
global {
    address dmz-net 192.168.150.0/24;
    address client-net 172.16.128.0/24;
    address web-servers 192.168.150.0/29;
}

[edit security policies]
user@host# show
from-zone trust to-zone dmz {
    policy p1 {
        match {
            source-address client-net;
            destination-address dmz-net;
            application [ junos-http junos-https ];
        }
        then {
            permit;
        }
    }
    policy p2 {
        match {
            source-address client-net;
            destination-address web-servers;
            application [ junos-http junos-https ];
        }
        then {
            deny;
        }
    }
    policy p3 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            deny;
        }
    }
}
global
    policy global-policy {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
}
```



Referring to the exhibit, what will happen if client 172.16.128.50 tries to connect to destination 192.168.150.3 using HTTP?

- A. The client will be denied by policy p2.
- B. The client will be permitted by the global policy.
- C. The client will be permitted by policy p1.
- D. The client will be denied by policy p3.

Correct Answer: C

[JN0-333 PDF Dumps](#)

[JN0-333 Practice Test](#)

[JN0-333 Study Guide](#)